

URL Filtering Policies

<https://campus.barracuda.com/doc/98210332/>

The CloudGen Firewall provides a predefined list of URL categories that are available for block listing and allow listing. The default action of a URL filtering policy can be either to block all URLs and define exceptions that are allowed, to allow all and define exceptions that are blocked, or to let the filter generate logs according to actions performed by users. You can change the default action for all URL policies individually.

URL Filtering Shared Policy Profiles							
Name	Origin	References	Description				
0 GlobURL	Local	1					

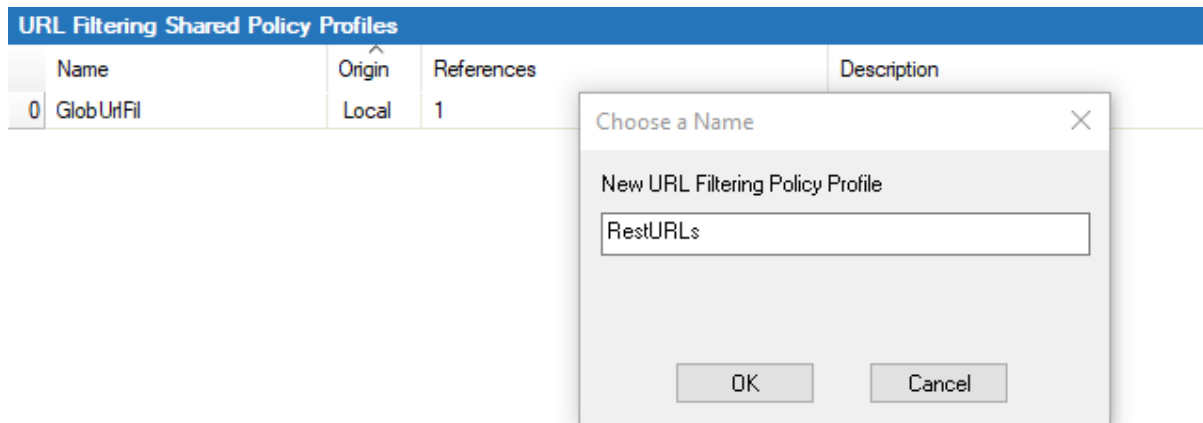
GlobURL							
URL Filtering		References					
Name	Description	Action	Source	User	URL Filter Match	Schedule	Safe Search Silent
0 BLOCK-ADS		Block	Any 0.0.0.0/0	Any	Advertisements or Banners	Always	Off No
1 WARN-DRUGS		Warn and Continue	Any 0.0.0.0/0	Any	Illegal Drugs	Always	Off N.A.
2 ALERT-WEAPONS		Alert	Any 0.0.0.0/0	Any	Terrorism or Extremists, Weapons, Violence or Suicide, Guns, Ammun...	Always	Off N.A.
3 SafeSearch		Allow	Any 0.0.0.0/0	Any	Any	Always	Off N.A.
4 URLLCatDefault	The default URLLCat policy. Only the action is modifiable.	Allow	Any 0.0.0.0/0	Any	Any	Always	Off N.A.

For information on how to customize default policy profiles, see [How to Configure Policy Profiles](#).

Create a URL Filtering Policy Profile

Create an explicit URL filtering policy profile to match individual requirements.

1. (On the Control Center) Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Global Firewall Objects/Policies**.
2. Click **Lock**.
3. In the left menu, expand **Policy Profiles**.
4. Select **URL Filtering**.
5. To add a new policy profile, click the plus icon (+) at the top right of the window, enter a profile name, and click **OK**.



6. Click **Send Changes** and **Activate**.

The policy profile now appears in the **URL Filtering Shared Policy Profiles** list, and you can create policies for it.

Create an Explicit URL Filtering Policy

1. (On the Control Center) Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Global Firewall Objects/Policies**.
2. (On a CloudGen Firewall) Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
3. Click **Lock**.
4. In the left menu, expand **Policy Profiles**.
5. Select **URL Filtering**. The URL filtering policies window opens.
6. (Control Center only) Select the profile you wish to create the policy for. The explicit policy list appears in the lower window.
7. (Control Center only) To add a new policy, click the plus icon (+) at the top right of the lower window. You can also right-click the list and select **Add Policy**.
(CloudGen Firewall only) To add a new policy, click the plus icon (+) at the top right. You can also right-click the list and select **Add Policy**.
8. Specify values for the following:
 - **Name** – Enter a descriptive name for the URL filtering policy.
 - **Description** – Enter a description.
 - **Action** – Select one of the following actions:
 - **Allow** – The CloudGen Firewall allows all URLs by default. Only URLs defined as exceptions will get blocked.
 - **Block** – The user is blocked from viewing the website and is redirected to the customizable URL filter block page. For more information, see [How to Configure Custom Block Pages and Texts](#).
 - **Warn and Continue** – Allows access to the URL. However, a warning page is shown. When a user clicks **Continue** in the browser, an entry is generated in the *Box/Firewall/Acknowledged* and *Box/Firewall/Alerted* log. The warning page is

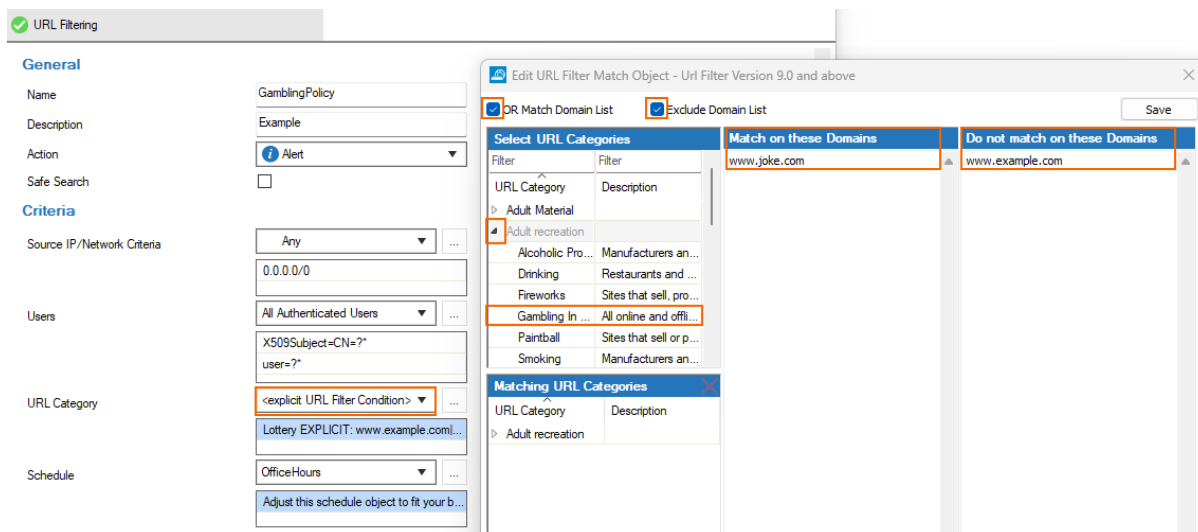
customizable. For more information, see [How to Configure Custom Block Pages and Texts](#).

For this action to apply, TLS Inspection must be enabled in the **Security Settings**. For more information, see [How to Configure Outbound TLS Inspection](#).

- **Alert** – Visiting a website in this category is silently logged. Go to **FIREWALL > Monitor, Filter Settings** and activate the filter for '**Warned**' to see the logged alerts.
- **Override** – Allows the user to request temporary access from an admin. Upon receiving the request, the override admin must log into the override admin interface to grant access for a specific amount of time to this otherwise blocked URL category. The admin can only grant overrides for the URL category, not for specific websites. For information on how to grant URL filter overrides, see [URL Filtering in the Firewall](#).
- **Safe Search** – Enable this check box to enforce Safe Search in browsers for the search engines Google, Yahoo, Bing, YouTube, and DuckDuckGo.

To use the Safe Search feature, TLS Inspection must be enabled in the **Security Settings**. For more information, see [How to Configure Outbound TLS Inspection](#).
- **Silent** – When selecting **Block** as the action, push notifications are generated whenever the policy applies. To avoid recurring pop-up windows, select the check box.

This setting only applies if the CloudGen Firewall acts as a point of entry for the Barracuda SecureEdge Agent. For more information, see the [Barracuda SecureEdge documentation](#).
- **Source IP/Network Criteria** – Select the source and destination network, or select **<Explicit Network>** and enter an IP address/network or a domain that gets resolved to an IP address for the matching.
- **URL Category** – Choose the categories you want to allow or block:
 - For common malware, select **Default**.
 - For individual categories:
 1. Select **explicit URL Filter Condition**.
 2. Either search or filter for the URL categories that you want to include in the object.
 3. Add the URL categories or subcategories (expand a category for a list) you wish to include in the object by clicking **+** next to an entry. The selected item appears in the lower section of the **Edit URL Filter Match Object** window.
 - To add an explicit URL, select **OR Match Domain List**.
 - To exclude an explicit URL, select **Exclude Domain List**.
- **Schedule** – Set a time schedule for the policy to apply. For more information, see [Schedule Objects](#).



General

Name: GamblingPolicy

Description: Example

Action: Alert

Safe Search: ☐

Source IP/Network Criteria: Any

Users: All Authenticated Users

URL Category: <explicit URL Filter Condition>

Schedule: OfficeHours

Edit URL Filter Match Object - Url Filter Version 9.0 and above

☒ OR Match Domain List ☐ Exclude Domain List

Select URL Categories

Filter	Filter
URL Category	Description
Adult Material	
Adult recreation	
Alcoholic Pro...	Manufacturers an...
Drinking	Restaurants and ...
Fireworks	Sites that sell, pro...
Gambling In ...	All online and offi...
Paintball	Sites that sell or p...
Smoking	Manufacturers an...

Matching URL Categories

URL Category	Description
Adult recreation	

Match on these Domains

www.joke.com

Do not match on these Domains

www.example.com

9. Click **OK**.
10. Click **Send Changes** and **Activate**.

The policy is now listed in the lower window and can be selected as **Policy** in your forwarding rules. For more information, see the last step in [How to Configure Policy Profiles](#).

Figures

1. url_overview.png
2. add_ico.png
3. url_new.png
4. add_ico.png
5. add_ico.png
6. url_filter_policy.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.